IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

CONNOR LAW, individually and on behalf of all others similarly situated; Plaintiff, v. EMS LINQ, LLC, Defendant.	Case No.: 1-24-cv-1533 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Connor Law ("Plaintiff") brings this Class Action Complaint against EMS LINQ, LLC ("LINQ" or "Defendant"), on behalf of himself individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including, but not limited to, Plaintiff's and Class Members' names, Social Security Numbers, and/or other personal information (collectively, "PII" or "Private Information").

2. LINQ is a Texas-based limited liability company that offers a variety of services to school districts, including human resource management.

3. Defendant was subject to a cyberattack between September 12, 2023 and May 13, 2024 (the "Data Breach"). Defendant investigated the Data Breach and determined that an unauthorized party gained access to certain LINQ-controlled databases containing the Private

Information of Plaintiff and other current and former employees of LINQ's clients.

4. On November 12, 2024, Defendant mailed Plaintiff a letter advising him that the data exposed in the Data Breach included Plaintiff's "name, Social Security number, date of birth and bank account information." Notice of Data Breach, Exhibit A hereto.

5. Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information was likely accessed by an unknown third party and precisely what type of information was accessed.

6. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant and thus Defendant was on notice that failing to take steps necessary to secure the Personal Information from those risks left that information in a dangerous condition.

7. Because of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

8. By obtaining, collecting, using, and profiting from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted Private Information was impacted during the Data Breach.

9. The exposed Private Information of Plaintiff and Class Members can—and likely will—be sold on the dark web. Indeed, Plaintiff's and Class Members' Private Information has likely already been published on the dark web.

10. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves.

11. This Private Information was compromised because of Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members.

12. Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their lifetimes.

13. Plaintiff brings this action on behalf of all persons whose Private Information was compromised because of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injuries because of Defendant's conduct. These injuries include:

(i) lost or diminished value of Private Information;

(ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

(iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time; and

(iv) the continued and exacerbated risk to their Private Information which:

a. remains unencrypted and available for unauthorized third parties to access and abuse; and

b. may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded. Defendant further disregarded their rights by failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures for the encryption of data, even for internal use.

16. Because of the Data Breach, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

17. Plaintiff Connor Law is a Citizen of Broomfield, Colorado. He received notice from Defendant that it lost control of his PII.

18. Defendant LINQ is a limited liability company formed under the laws of Delaware and having its corporate office at 2801 Via Fortuna, Suite 400, Austin, Texas, 78746.

19. Defendant's registered agent is Corporation Service Company, located at 251 Little Falls Drive, Wilmington, Delaware, 19808.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of

interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has general personal jurisdiction over Defendant because Defendant is based and operates in the Western District of Texas.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(l) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

IV. FACTUAL ALLEGATIONS

The Data Breach

23. In the ordinary course of providing human resources services to its clients, LINQ obtained a variety of sensitive, personal and private information regarding its clients' current and former employees, including Plaintiff and Class Members.

24. Among Defendant's clients was The Academy of Charter Schools, a public school in Westminster Colorado and Plaintiff's former employer.

25. Upon information and belief, in the course of collecting Private Information from its clients' employees, Defendant promised to provide confidentiality and adequate security for the data it collected from its clients' employees.

26. In a "Security Statement" on its website, Defendant states that "Security is a key priority at LINQ," and claims to have "implemented policies, procedures, and technical controls to ensure that access to Customer Data is managed on a 'need to know basis,' that LINQ personnel appropriately protect their access, and that information is accessed securely."[1]

[1] Defendant LINQ, "Security Statement," available at https://www.linq.com/legal/security-statement/ (last accessed December 12, 2024).

27. Defendant had obligations created by contract, industry standards, common law, and representations made to its clients and to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

28. Defendant agreed to and undertook legal duties to maintain the protected Private Information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

29. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

30. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the education and financial sectors preceding the date of the breach.

32. As reported by the Identity Theft Resource Center, in 2023 a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[2] Of the 2023 recorded data breaches, 173 were in the education industry and 744 were in the financial services industry.[3]

33. Therefore, the increase in such attacks, and attendant risk of future attacks, was

[2] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (*last accessed* December 13, 2024).
[3] *Id.*

widely known to the public and to anyone in Defendant's industry, including Defendant.

34. In its notice letter (Exhibit A), Defendant describes the data breach as follows:

> **What Happened?** LINQ recently became aware of suspicious activity in one of our cloud solutions that supports our school district customers. We took immediate steps to confirm the security of this system and began an investigation with the assistance of third-party cybersecurity experts. On October 11, 2024, our investigation determined that an unauthorized user accessed the solution for brief intermittent periods of time between September 12, 2023, and May 13, 2024 an may have obtained certain information, including that which we received in connection with the services LINQ provides to The Academy.
>
> **What Information Was Involved?** We conducted a thorough review of the involved information and determined that it may have included your name, Social Security number, date of birth and bank account information.

35. As a consequence of the unauthorized access to Defendant's computer network, Plaintiff's and Class Members' Private Information was exposed to cybercriminals.

36. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

37. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for its intended purposes only, and to make only authorized disclosure of this Private Information.

38. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information, which includes Social Security numbers, information that is static, does not change, and can be used to commit myriad financial crimes.

39. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing

the exposure of Private Information.

41. Because of Defendant's failure to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, an unauthorized third party infiltrated Defendant's systems and stole Plaintiff's and Class Members' Private Information.

42. The unencrypted PII of Plaintiff and Class Members will likely end up for sale on the dark web, as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

Plaintiff's Experience

43. Plaintiff received a notice from Defendant on or around November 12, 2024, that his Private Information was accessed in the Data Breach.

44. Plaintiff is a former employee of The Academy of Charter Schools, a public school in Westminster, Colorado.

45. Plaintiff, through his employer, provided Defendant with certain Private Information as a necessary part of receiving his pay and benefits.

46. Plaintiff is careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

47. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his sensitive online accounts.

48. Because of the Data Breach, Defendant advised Plaintiff to take certain steps to

protect his Private Information and otherwise mitigate his damages.

49. Because of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. And this time was spent at Defendant's direction by way of the Data Breach notice where Defendant recommended that Plaintiff mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

50. Even with the best response, the harm caused to Plaintiff cannot be undone.

51. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

52. Plaintiff has suffered imminent and impending injury arising from the exacerbated risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

53. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Defendant Failed to Comply with FTC Guidelines

54. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[4] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[5]

56. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect client data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

[4] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 19, 2024).
[5] *Id*.

58. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to account holders' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Defendant was always fully aware of its obligation to protect the PII of its clients and account holders. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

60. As shown above, experts studying cyber security routinely identify educators and financial services providers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

61. Several best practices have been identified that at a minimum should be implemented by professional service providers like Defendant, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, antivirus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

62. Other best cybersecurity practices that are standard in the financial services sector include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

63. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

64. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Breach of Duty

65. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect account holders' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train employees in the proper email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section *5* of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

66. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing malignant computer code, and inadequately trained employees who shared their email credentials with cybercriminals, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

67. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

The Risks to Plaintiff and Class Members Created by Defendant's Failure to Safeguard Private Information

68. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

69. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

70. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and

is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

71. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

72. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

73. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

74. One such example of criminals using PII for profit is the development of "Fullz" packages.

75. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

76. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that

Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

77. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims, and the numbers are only rising.

78. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

79. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

80. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

81. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

82. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and

amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."

83. The FTC has also issued Many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed;

(4) limiting administrative access to business systems;

(5) using industry-tested and accepted methods for securing data;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.

84. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

85. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiff's and Class Members' Damages

86. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

87. The credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden on Plaintiff and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

88. Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

89. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

90. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

91. Plaintiff was damaged in that his Private Information is in the hands of cyber criminals.

92. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

93. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

94. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

95. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

96. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

97. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

98. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

99. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

100. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

101. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

V. CLASS ACTION ALLEGATIONS

102. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

103. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the 2023-24 Data Breach (the "Class").**

104. Excluded from the Class are Defendant's officers and directors, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the

Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

105. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery.

106. Numerosity. The Members of the Class are so numerous that joinder of all of them in a single proceeding is impracticable. The exact number of Class Members is unknown to Plaintiff now, but Defendant's notice letter states the data compromised included data "received in connection with the services LINQ provides to The Academy," a school with 250 staff.[6] Moreover, Defendant advertises on its website that it processes payroll for 364,000 employees.[7]

107. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

[6] The Academy of Charter Schools, "About Us," https://www.theacademyk12.org/about-us (last visited December 12, 2024).
[7] Defendant LINQ, https://www.linq.com/ (last visited December 12, 2024).

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant failed to provide notice of the Data Breach promptly; and

j. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

108. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

109. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

110. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

111. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy.

112. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

113. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

114. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

115. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

116. Defendant requires its clients' employees, including Plaintiff and Class Members, to submit non-public personal information in the ordinary course of providing its services.

117. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's

duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

118. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

119. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

120. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

121. Defendant further had a duty to use reasonable care in protecting confidential data because Defendant is bound by industry standards to protect confidential Private Information.

122. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect timely that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

123. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

124. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

125. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

126. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

127. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and All Class Members)

128. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

129. Defendant entered into written contracts with its clients, including The Academy of Charter Schools, to provide human resources services.

130. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and Class Members and to timely and adequately notify them of any Data Breach.

131. These contracts were made expressly for the benefit of Plaintiff and Class Members, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, its clients' employees—Plaintiff and Class Members—would be harmed.

132. Defendant breached the contracts it entered into with its clients by, among other things, (i) failing to use reasonable data security measures, (ii) failing to implement adequate protocols and employee training sufficient to protect Plaintiff's PII from unauthorized disclosure to third parties, and (iii) failing to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

133. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result of Defendant's breach.

134. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

THIRD COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

135. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

136. In the alternative to Plaintiff's claim for Breach of Third-Party Beneficiary Contract, when Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

137. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

138. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and adhered to industry standards.

139. Plaintiff and Class Members entrusted their retirement funds and attendant data to Defendant with the reasonable belief and expectation that Defendant would provide adequate data security. Defendant failed to do so.

140. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

141. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

142. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

143. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

144. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

145. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

146. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and All Class Members)

147. Plaintiff re-alleges and incorporate the above allegations as if fully set forth herein.

148. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

149. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

150. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

151. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

152. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

by failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

153. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and his counsel to represent the Class, and finding that Plaintiff is a proper representatives of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For an Order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Any other relief that this court may deem just and proper.

VIII. JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Date: December 13, 2024,

Respectfully submitted,

/s/ Jarrett L. Ellzey

Jarrett L. Ellzey
Texas Bar No. 24040864
jellzey@eksm.com
Leigh S. Montgomery
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF AND THOSE SIMILARLY SITUATED